## ABSTRACT

A password is split into a plurality of pieces. The pieces are stored at different remote servers. The different remote servers have the property that together they can determine that the user has knowledge of the correct password. If any subset of the servers are compromised, the compromised subset cannot convince any remaining servers that they know the password.